计算机科学
COMPUTER SCIENCE

面向语音助手的窃听攻击与防御研究现状与挑战

黄文斌，任炬，曹航程，蒋洪波，熊礼治，陈先意，付章杰

引用本文

黄文斌，任炬，曹航程，蒋洪波，熊礼治，陈先意，付章杰. 面向语音助手的窃听攻击与防御研究现状与挑战[J]. 计算机科学，2025，52(11)：364-372.

HUANG Wenbin, REN Ju, CAO Hangcheng, JIANG Hongbo, XIONG Lizhi, CHEN Xianyi, FU Zhangjie. Research Status and Challenges of Eavesdropping Attacks and Defenses Targeting VoiceAssistants [J]. Computer Science, 2025, 52(11): 364-372.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.250300047

面向语音助手的窃听攻击与防御研究现状与挑战

黄文斌[1,2]　任　炬[3]　曹航程[4]　蒋洪波[5]　熊礼治[1]　陈先意[1]　付章杰[1]
1 南京信息工程大学计算机学院、网络空间安全学院　南京 210044
2 浙江大学区块链与数据安全全国重点实验室　杭州 310027
3 清华大学计算机科学与技术系　北京 100084
4 香港城市大学计算机科学系　香港 999077
5 湖南大学信息科学与工程学院　长沙 410082
(wenbinhuang@nuist.edu.cn)

摘　要　语音助手作为人机语音交互的便捷接口,已在居家、运动、车载等诸多场景中得到广泛应用,为医疗、金融、教育等产业的智能化升级提供了有力支持。然而,语音助手的便捷与普及也引发了严峻的窃听用户对话,从而造成用户隐私泄露的问题。现有关于语音助手的综述性文献主要聚焦于语音欺骗攻击与防御、对抗样本攻击与防御等方面,针对语音窃听攻击与防御的总结与分析仍有待完善。为此,深入研究了面向语音助手的窃听攻击与防御,并对现有研究进行了详细综述。首先,全面回顾并深入分析了当前存在的窃听攻击方法,根据窃听攻击实现方式的不同进行分类,并对攻击的实施手段、攻击目标、所需技术和权限、攻击的隐蔽性等进行了详细的探讨,旨在全面了解语音助手面临的潜在威胁。其次,对近年来防御语音助手窃听攻击的研究工作进行了系统梳理,通过对不同防御技术的分类总结,结合其应用场景和检测效果进行深入分析,总结了防御方法存在的不足与面临的挑战,为进一步提升语音助手的安全性提供了有益参考。最后,对窃听攻击和防御领域面临的主要研究挑战进行了详细分析,并探讨了未来可能的研究方向。

关键词:语音助手安全;语音窃听攻击;语音窃听防御
中图分类号　TP393

Research Status and Challenges of Eavesdropping Attacks and Defenses Targeting Voice Assistants

HUANG Wenbin[1,2],REN Ju[3],CAO Hangcheng[4],JIANG Hongbo[5],XIONG Lizhi[1],CHEN Xianyi[1] and FU Zhangjie[1]
1 School of Computer Science,School of Cyber Science and Engineering,Nanjing University of Information Science and Technology,Nanjing 210044,China
2 The State Key Laboratory of Blockchain and Data Security,Zhejiang University,Hangzhou 310027,China
3 Department of Computer Science and Technology,Tsinghua University,Beijing 100084,China
4 Department of Computer Science,City University of Hong Kong,Hong Kong 999077,China
5 College of Computer Science and Electronics Engineering,Hunan University,Changsha 410082,China

Abstract　Voice assistants serve as convenient interfaces for human-computer voice interaction,finding widespread application across various settings including homes,sports,and vehicles. They play a pivotal role in facilitating the intelligent advancement of industries,such as healthcare,finance,and education. However,the widespread adoption and convenience of voice assistants have also precipitated significant concerns regarding the eavesdropping on user conversations,consequently leading issues of user privacy disclosure. Existing literature primarily focuses on voice spoofing attacks and defenses,as well as adversarial sample attacks and defenses. However,there remains a notable gap in the analysis and synthesis of voice eavesdropping attacks and defenses. To address this gap,this work delves deeply into the mechanisms of eavesdropping attacks on voice assistants and meticulously reviews existing research in this domain. Firstly,this work conducts a comprehensive review and in-depth analysis of various eavesdropping attack methods,categorizs them based on their implementation strategies. It explores the means of attack,targets,neces-

到稿日期:2025-03-10　返修日期:2025-04-28
基金项目:江苏省基础研究计划自然科学基金(BK20240694);国家自然科学基金(62502218);浙江大学区块链与数据安全全国重点实验室开放课题(A2530);南京信息工程大学人才启动经费(2024r045);江苏省重大专项(BG2024042)
This work was supported by the Natural Science Foundation of Jiangsu Province,China(BK20240694),National Natural Science Foundation of China(62502218),Open Research Fund of the State Key Laboratory of Blockchain and Data Security,Zhejiang University(A2530),Startup Foundation for Introducing Talent of NUIST(2024r045) and Jiangsu Provincial Science and Technology Major Project(BG2024042).
通信作者:熊礼治(lzxiong16@163.com)

sary technology and permissions，and concealment techniques employed，aiming to provide a comprehensive understanding of the potential threats faced by voice assistants. Secondly，recent research efforts aimed at defending against voice assistant eavesdropping attacks are systematically reviewed. Through the classification and summarization of different defense technologies，coupled with insights into their application scenarios and detection effectiveness，the paper highlights the shortcomings and challenges of existing defense mechanisms，thereby offering valuable insights for enhancing the security of voice assistants. Lastly，this study meticulously analyzes the primary research challenges in the realm of eavesdropping attacks and defenses，while also discussing potential future research directions. By identifying these challenges and proposing future avenues of exploration，the paper aims to guide ongoing research endeavors towards bolstering the resilience of voice assistant systems against eavesdropping threats.

Keywords Voice assistant security，Voice eavesdropping attacks，Voice eavesdropping defense

1 引言

在当今数字化时代，人工智能技术的迅猛发展深刻改变了人机互动的方式[1-3]。其中，作为人机交互领域的一项创新技术，语音助手凭借方便且高效的特性正逐渐成为人们日常生活中不可或缺的一部分。语音助手不仅在智能手机上得到广泛应用，而且其提供的服务还涉及智能家居、车载系统、可穿戴设备等诸多领域[4-7]。根据 Grand View Research 的报告，2022 年语音助手的市场规模为 144.2 亿美元，且在 2022 年至 2030 年期间将以 15.3%的年复合增长率持续增长[8]。

语音助手的工作机制如图 1 所示，包含用户唤醒和用户操控两部分。具体而言，语音助手的初始状态为待机状态，只有在捕捉到用户发出的预设唤醒词（例如，Hey Siri、小爱同学、OK Google）时才能被激活。激活后，用户可以通过语音指令操控设备进行通话、发送信息、设置闹钟等操作，实现非接触式人机交互[9-10]。

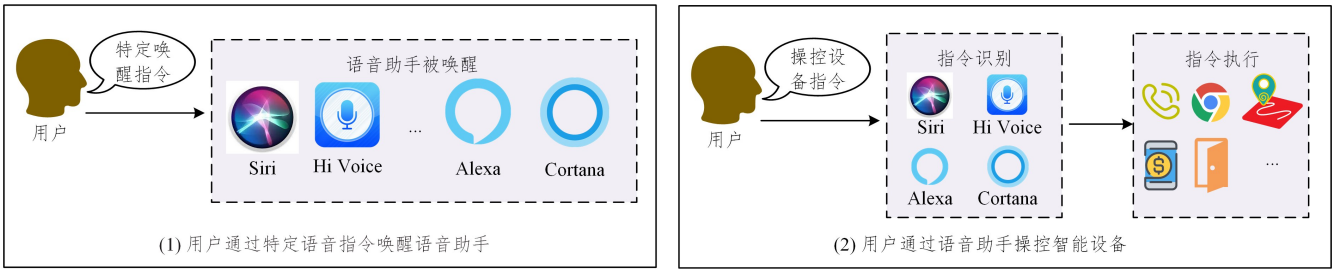

图 1 语音助手的工作流程

Fig. 1 Workflow of voice assistants

尽管语音助手提供了高效、自然、便捷的语音交互，但其广泛使用也引发了严峻的安全和隐私问题，即语音助手会在无用户唤醒的前提下自动激活，窃听用户对话，造成用户隐私泄露。早在 2019 年，英国《卫报》就报道了“苹果承包商在 Siri 对话中听到秘密信息”的问题[11]。该报道称，苹果公司在未明确说明的情况下使用 Siri 录制用户的私密对话并转交给承包商进行分析。同时，比利时-荷兰语国家广播公司也报道称，谷歌会窃听用户与谷歌助手的对话[12]。近年来，越来越多的人在网上发表声明，他们声称在手机能听到的范围内所谈论的话题或商品会出现在有针对性的网络广告中，这引发了人们对私人谈话被秘密记录和分析的担忧[13-14]。

为了验证智能设备的语音助手是否存在窃听行为，Cheng 等[15]测试了多个亚马逊（Amazon）设备。通过启用和禁用设备的麦克风发现，Alexa 应用程序日志和亚马逊的语音服务网络流量之间存在不一致性。这一结果论证了亚马逊的 Echo Dot 设备会在无用户唤醒的情况下窃听私人对话，并将对话上传到亚马逊的云平台进行分析。Edu 等[16]也发现了这一现象，并证实了语音助手的窃听行为是客观存在的。此外，Qin 等[17]利用语音感知技术对语音助手进行分析，发现语音助手不仅会在无用户发出唤醒指令时记录用户声音，而且会持续观察周围环境中的对话和典型噪声。

尽管已有研究验证了语音助手窃听攻击的可行性和危害性，并提出了一系列防御方案，但目前关于语音助手的综述性文献[18-20]主要聚焦于针对语音助手所面临的欺骗攻击与防御[21-22]、对抗样本攻击与防御[23-24]等，而针对语音助手的窃听攻击与防御研究的系统性综述仍有待完善。因此，本文将深入探讨语音助手的窃听攻击与防御的研究现状与挑战，以系统性地回顾当前的研究成果，并对未来的发展方向提出展望。首先，通过概述语音助手的工作机制，揭露语音助手存在的隐私泄露风险，并对现有的窃听攻击的实施方式及已有研究进行分类与总结。其次，依据防御语音助手窃听攻击所采用的主要原理，对现有的窃听防御研究工作进行了详细的分析和讨论。最后，讨论了揭露语音助手的安全和隐私漏洞以及抵御语音助手窃听攻击所面临的主要挑战，并展望该领域未来的研究焦点。

通过对语音助手窃听攻击与防护的深入研究，本文旨在为学术界、产业界和政策制定者提供有价值的参考，以期推动语音助手技术在更为安全、可信的环境下发展，从而更好地满足用户需求，最终建立一个可持续且健康的语音助手生态系统。

本文第 2 章介绍了语音窃听攻击的研究现状、存在的问题及挑战；第 3 章介绍了语音窃听防御的研究现状及存在的主要研究挑战；第 4 章展望了未来的研究方向；最后总结全文。

2 语音窃听攻击问题的研究现状及挑战

语音窃听攻击的目的是在用户未发出唤醒指令的情况下，恶意激活语音助手，以窃听用户的对话。为实现这一目标，现有研究采取了各种方式，依据窃听攻击的实施方式主要可归纳为以下 3 类：基于语音助手恶意操控的窃听攻击、基于侧信道的窃听攻击和基于第三方应用的窃听攻击。对这 3 种攻击的详细分析如表 1 所列。

表 1 不同语音窃听攻击类型的全面比较

Table 1 Comprehensive comparison of different types of voice eavesdropping attacks

攻击类型	相关工作	攻击目标	主要技术	所需条件	所需权限	影响范围	隐蔽性
基于语音助手恶意操控的窃听攻击[25-28]	Jang[25]	访问性接口	音频输入输出技术	—	扬声器访问权限	搭载语音助手的智能设备	低
	Zhang[26]		语音克隆技术、机器学习技术		麦克风和扬声器访问权限		中
	Esposito[27]		无线通信、音频输入输出技术	无线连接	文件传输权限		低
	Huang[28]		进程监听、修改、重放技术	设备的注入框架支持	进程访问权限		高
基于侧信道的语音窃听攻击[29-34]	Zhang[29]	麦克风硬件	调频技术、超声发射技术	超声发射器	—	配备麦克风、扬声器以及零权限传感器的智能设备	高
	Roy[30]		频带划分技术、超声发射技术				
	Michalevsky[31]	陀螺仪	信号恢复技术、深度学习技术	振动信号采集器			
	Ba[32]	加速度计		—			
	Gao[33]	加速度计和陀螺仪					
	Wang[34]	加速度计、陀螺仪和磁力计	信号恢复技术				
基于第三方应用的语音窃听攻击[40-42]	Diao[40]	Google Voice Search API	安卓开发技术	—	恶意注入和麦克风访问权限	安装应用程序的智能设备	高
	Zhang[41]	原生开发应用程序	移动应用开发技术				
	Huang[42]	未加固应用程序	反编译技术				

2.1 基于语音助手恶意操控的窃听攻击

依据语音助手的工作机制，语音助手只有在捕获到用户说出特定的唤醒词后，才能够启动并聆听用户对话。然而，语音助手可能存在未经用户唤醒的前提下，私自启动并窃听用户对话的问题。攻击者可以通过操控设备自播放唤醒指令、恶意事件重放等方式，来操控语音助手实现窃听攻击。攻击的概述流程图如图 2 所示。

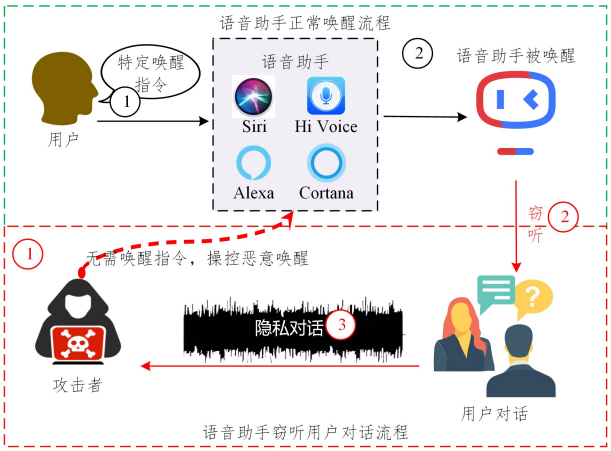

图 2 基于语音助手恶意操控的窃听攻击概述图

Fig. 2 Overview of eavesdropping attacks based on malicious manipulation of voice assistants

由于语音助手的唤醒需要特定的语音指令，Jang 等[25]的研究论证了语音助手存在可以被设备自发出语音指令唤醒的漏洞。基于此，一些研究通过设备自播放音频的方式唤醒语音助手，进而实施窃听攻击。为了绕过语音助手的身份认证机制，Zhang 等[26]首先通过第三方应用程序收集用户音频，并利用深度学习算法合成虚假唤醒指令。通过扬声器播放实现恶意唤醒，操控语音助手进行窃听。对于无身份认证机制的智能家居设备（如智能音箱等），Esposito 等[27]发现 Echo 设备上运行的 Alexa 利用设备自身播放的音频文件的漏洞，通过蓝牙或者无线电台将音频文件传输到设备后，再操控扬声器播放音频，便可唤醒语音助手实现窃听攻击。

然而，音频播放的攻击方式很容易被用户感知，因此窃听攻击实施的隐蔽性不足。为了实现无需音频播放的语音助手恶意唤醒，Huang 等[28]通过分析语音助手的工作机制，提出了基于事件重放的攻击方法。该方法通过捕获、重放唤醒事件并生成恶意意图，来达到无需音频的语音助手唤醒。这一方法虽然提升了攻击的隐蔽性，但是需要获取攻击设备的物理权限以及 root 权限，因此攻击实施难度较高。

2.2 基于侧信道的窃听攻击

一些研究通过对智能设备传感器实施攻击来捕获并恢复用户语音[29-37]。例如，利用麦克风的非线性特征实施海豚攻击，恢复加速度计、陀螺仪等零权限传感器所捕获到的麦克风或扬声器的振动信号等。基于侧信道的窃听攻击概述如图 3 所示。

Zhang 等[29]提出的海豚攻击是著名的侧信道攻击。该攻击依据麦克风硬件的非线性漏洞，利用调频技术在超声波载体上调制可听的语音命令，使命令信号无法被人类感知，但可以被语音助手正确理解。此时，攻击者便可以在不直接访问设备的情况下，操控语音助手窃听用户对话、窃取用户隐私。实验结果表明，海豚攻击可以成功攻击大多数的语音助手，包括 Siri，Google Now，Samsung S Voice，Huawei Hi

Voice，Cortana 和 Alexa 等。然而，这类攻击只能在 1.5 m 范围内实施。

为了扩大攻击范围，Roy 等[30]设计了一种替代的发射机，打破了距离和可听性之间的零和博弈，将攻击范围拓展至 7.6 m。具体操作是使用多个扬声器组成一个由放大器驱动的超声波扬声器阵列，并使语音信号的条带段穿过该阵列，成功实施了对亚马逊 Echo，iPhone Siri 和三星设备的远距离控制。

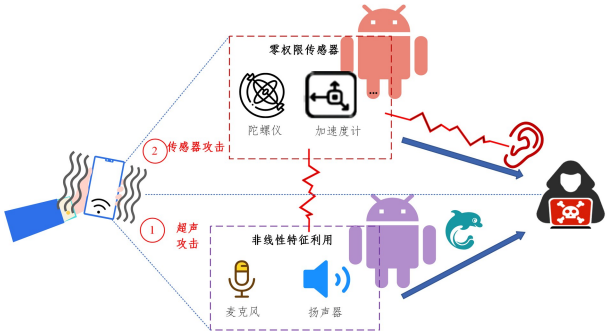

图 3 基于侧信道的语音窃听攻击概述图

Fig. 3 Overview of side channel-based voice eavesdropping attacks

除了通过侧信道激活语音助手进行窃听攻击外，由于智能设备配备了丰富的传感器来采集信息，一些研究根据运动传感器对声波产生的振动较为敏感的特点，通过零访问权限的运动传感器作为侧信道，实现隐蔽的语音窃听。

Michalevsky 等[31]依据运动传感器能够接收通过固体介质传播的语音信号的特点，利用智能手机的陀螺仪来拾取由放置在同一张桌子上的独立扬声器引起的表面振动。在捕获振动信号后，通过信号处理和机器学习技术进行分析，可以识别扬声器播放的语音信息。然而，这一工作存在两个主要限制：1）需要外置设备采集攻击信号；2）由于采样上限为 200 Hz，因此这些传感器只能拾取窄带（85～100 Hz）的语音信号。

为突破上述限制，基于同一设备的运动传感器和扬声器将始终与同一电路板保持物理接触且彼此非常接近物理事实，Ba 等[32]通过实验发现语音信号在加速度计测量中始终产生显著的响应，据此提出了 AccelEve 攻击。基于加速计能够捕获 85～250 Hz 范围内的语音信息，他们设计了一种新颖的基于深度学习的系统，通过学习从加速信号的频谱图表示中识别和重建的语音信息，从而达到窃听的目的。

不同于上述只采用单个运动传感器实施窃听攻击，Gao 等[33]提出了 InertiEAR 攻击。该攻击利用加速度计和陀螺仪共同窃听智能手机的顶部和底部扬声器，即使是在低于 200 Hz 的采样信号中仍然可以分析出足够的信息。实验结果表明，IntertiEAR 在低频采样率下的识别准确率达到 78%，并且还可以实现跨设备攻击，在 12 款智能手机上的跨设备准确率高达 60.9%。

尽管上述研究都证明了使用内置传感器窃听扬声器播放的声音的可行性，但是他们都是基于数据驱动方法，即需要采集大规模的语音传感器测量样本来训练识别与重构模型。然而，由于严重的隐私问题，这些数据是不可公开的。为解决该问题，Wang 等[34]提出了无需训练的内置扬声器窃听攻击方法 VoiceListener。其基本思想是利用模型驱动的方法，通过内置传感器发现语音泄露侧通道，并从欠采样传感器测量中恢复语音。具体而言，他们开发了一种混叠校正的超分辨率机制，包括基于混叠的音高估计和混叠校正的语音恢复，将欠采样窄带传感器测量值转换为宽带语音。该方法不需要收集数据，可以跨越不同的声音、平台和领域实施窃听攻击，但实施该攻击需要精准的信号设计，无法大规模部署。

2.3 基于第三方应用的窃听攻击

数以万计的移动应用程序被开发出来，为用户提供丰富的功能服务。但恶意软件会在未经用户授权的情况下，私自访问麦克风从而窃听用户对话，该问题已引发重要关注[38-39]。其攻击的概述流程如图 4 所示。

图 4 基于第三方应用的窃听攻击概述图

Fig. 4 Overview of application-based voice eavesdropping attacks

Diao 等[40]开发了一个包含攻击模块的恶意软件 VoicEmployer。该软件被安装和启用后，便可以在无需任何许可的情况下直接调用 Android Intent 机制，将内置的 Google 语音助手模块带到前台，实现对用户对话的窃听。虽然在 Samsung Galaxy S3，Meizu MX2 和 Motorora A953 上成功实施了攻击，但是由于 Google 生态系统独特的 API 需求，这些攻击方法很容易被检测到。

除了操控语音助手，一些攻击通过开发恶意软件或应用程序来窃听用户对话。Zhang 等[41]开发了一款概念验证间谍软件，并将其伪装成一款流行的麦克风控制游戏应用程序，以便合理地要求访问麦克风的权限。该恶意软件会在用户使用时偷偷记录用户对话并进行分析，实验表明它能达到 97% 以上的窃听成功率。

除直接开发恶意应用程序外，Huang 等[42]通过将恶意程序注入第三方应用程序的方式，开发了恶意应用程序 iEarSpy。iEarSpy 能够在未经用户授权的前提下，实现对麦克风的直接访问，达到窃听用户对话的目的。虽然在不同品牌、不同型号且搭载不同安卓系统版本的智能设备上验证了该窃听攻击的可行性，但由于受到应用商店和系统安全策略的限制，该程序可能被检测和阻止。此外，注入攻击的方式只适用于未经加固处理的应用程序。

2.4 存在的不足及挑战

虽然已有研究通过多种方式实现窃听攻击，以此揭露语音助手的隐私风险，但这些攻击仍存在攻击行为明显、攻击实施难度高和攻击范围受限等主要局限。

1）攻击隐蔽性不足：通过语音命令唤醒语音助手的非法行为，不仅容易被用户感知，且恶意调用扬声器播放音频的行

为也很容易被现有的安全保护方案识别，因此攻击的隐蔽性不足。

2）攻击实施难度高：基于侧信道的方法虽然可以实现极隐蔽的窃听攻击，但该攻击的实施需要精准的信号设计，且易受到环境的影响，因此此类攻击在现实中无法被大规模部署。

3）攻击通用性不足：虽然基于第三方应用程序的方法可以在较低的实施难度下实施隐蔽的窃听攻击，但这些攻击往往针对特定的语音助手，比如智能家居设备中的语音助手、应用程序的语助手或谷歌语音助手。

通过上述分析可以发现，恶意的攻击者能否操纵不同类型设备的语音助手实现隐蔽的窃听，是探索语音助手安全与隐私漏洞的重要研究挑战。

3 窃听防御研究现状及挑战

前文介绍了各种类型的语音窃听攻击后，本章将聚焦于国内外研究学者提出的窃听防御方法。总体而言，根据语音助手在提供语音交互功能时需要网络连接的前提条件和窃听攻击的可能实施方式，窃听防御方法主要分为基于流量分析的方法、基于侧信道的方法、基于源码审查的方法以及基于麦克风状态显示的方法。本文对这些方法进行了简要的总结与对比，并对方案的有效性进行了分析，结果如表 2 所列。

表 2 语音窃听攻击的防御方法

Table 2 Defense schemes of voice eavesdropping attacks

窃听检测方案类别	相关工作	应用场景	方案有效性
基于流量分析的方法[43-46]	Wang[43]，Ahmed[45] Mitev[46]，Zhou[44]	移动应用程序 智能家居设备	高
基于侧信道的方法[47-48]	Zhu[47] Sun[48]	移动应用程序 智能家居设备	中
基于源码审查的方法[49-54]	Zhao[49]，Meng[50]，Fratantonio[51]，Senanayake[52]，Xu[53]，Wong[54]	移动应用程序	低
基于麦克风状态显示的方法[55-58]	Lee[55]，Wang[56]，Zouhaier[57]，Huang[58]	配备屏幕的智能设备	低

3.1 基于流量分析的方法

Wang 等[43]提出了分析系统 LeakDoctor，通过将网络流量的动态响应差异分析与静态响应污染分析相结合，实现对应用程序窃听用户对话的自动诊断。依据应用程序获取用户对话是为了直接或间接的提供功能服务的观察结果，LeakDoctor 对应用程序分别进行动态和静态分析。在动态分析方面，LeakDoctor 在运行时主动修改泄露的私有数据的值，并观察这些值对远程响应的影响，以确定它们是否影响应用程序的功能。在静态分析方面，LeakDoctor 试图将每个隐私泄露与应用程序的特定功能联系起来，以确定它是否服务于应用。当它确实服务于某些功能时，则当前获取用户对话是合理的，否则它是不合理的，被认为是窃听。LeakDoctor 虽然在评估 1 060 个应用程序的时，可以自动判断出 71.9% 的隐私泄露情况，但是其只能识别不提供语音服务的应用程序的窃听行为，当提供语音服务的应用程序存在窃听用户对话时，LeakDoctor 会产生极高的漏报率。

Mitev 等[46]提出了 LeakyPick 架构，其主要组成部分为可以放置在家中任意位置的探测装置。该探测装置通过向附近发射音频探针，检测具备传输音频到互联网的智能家居设备。随后，LeakyPick 使用流量爆发分析和统计探测的方法，准确识别包含音频的网络流。首先，通过对支持麦克风的物联网设备在传输音频时的调用过程和数据通信行为进行分析，发现设备在正常待机操作期间通常不会发送太多流量。基于这一特性，LeakyPick 将来自设备的网络流量划分为特定大小的时间窗口，并计算每个时间窗口中的平均流量速率。结果表明，当流量速率为 23 kbit/s 时，可有效地将音频突发从背景流量中分离出来。其次，为了排除非音频传输导致的流量突发情况，LeakyPick 使用统计探测来改进音频传输检测。它首先记录每个智能家居设备空闲时的流量并将其作为基线流量；然后使用独立的双样本 t 检验来比较设备空闲时的网络流量分布特征和设备在音频通信时的流量分布特征，通过分布匹配来识别窃听导致的音频流量。在树莓派上搭建系统并进行窃听检测，实验结果表明，在检测 8 个具有语音助手功能的设备的音频传输时，测量精度达到 94%。

上述统计的方法虽然可以在保证与机器学习方法相同性能的同时，去除机器学习方法需要设备先验知识进行模型训练的过程，但是这类方法只适用于网络上传流量单一的智能家居设备，对于网络流量环境复杂的移动设备，则难以适用。

3.2 基于侧信道的方法

Zhu 等[47]提出了应用级的窃听防御系统 PhoneCheck。该系统由权限分析和窃听检测两部分组成。在权限分析模块，通过对智能设备上第三方应用程序的特性权限进行详尽的分析，根据麒麟安全规则制定更为多元化的安全规则，过滤具有可疑权限组的应用作为目标；在确定可疑目标后，窃听检测模块会在目标应用启动时密切关注目标的侧信道信息，例如 CPU 消耗和网络数据使用情况，以此推断应用程序是否存在窃听行为。然而，应用程序的窃听行为不一定会导致手机状态发生变化，此时窃听将无法被该系统防御。

不同于上述工作分析设备的硬件设备，Sun 等[48]提出了一种新的选择性干扰系统 MicShield。该系统通过向语音助手发射干扰信号来混淆用户的私人语音，使语音助手所窃听到的语音无法正确被解析。具体而言，MicShield 会在离线状态下持续监听周围环境的声音，并不断发出干扰信号，使得语音助手无法正确解析所窃听的用户对话内容。但当 MicShield 感知到特定的唤醒词后，会立即停止干扰。此外，MicShield 的离线工作状态确保了其不受始终监听、云操作的虚拟网关带来的隐私风险的影响。

MicShield 虽然可以使语音识别算法只能识别不足 1% 的隐私对话内容，但是受限于干扰信号的播放，使得其仅适用于智能家居设备，无法抵御移动设备面临的窃听困扰。

3.3 基于源码审查的方法

由于窃听行为可能是由恶意应用程序或设备存在隐藏的后门引起的，许多研究者提出检查是否存在后门，以判断语音助手是否会窃听用户对话。Zhao 等[49]提出了一种静态分析

技术 INPUTSCOPE，用于自动发现移动应用程序中的隐藏功能。该技术利用移动应用程序处理和响应用户输入数据的方式，其流程主要包含以下 3 个步骤。首先，INPUTSCOPE 将 Android 移动应用程序作为输入，以确定输入应用程序何时将用户输入的数据与存储在应用程序中或通过网络检索的某些值进行比较。然后，INPUTSCOPE 通过引入用户输入验证执行上下文的新概念来暴露输入触发的秘密，该概念结合了输入验证过程的两个正交方面：1）被验证的数据的类型；2）与比较结果相关的代码分派行为，例如迭代验证的次数和成功验证后潜在分支的数量。最后，INPUTSCOPE 在一组安全策略的帮助下检查内容和执行上下文，以揭露移动应用程序中隐藏的后门。

Meng 等[50]提出了 AppAngio 系统，该系统通过 API 级审计日志揭示 Android 应用程序行为中的上下文信息，进而识别应用程序的后门行为。AppAngio 系统主要由两个模块构成。1）日志模块：该模块部署在用户的 Android 设备或配置的模拟器上，用于捕获目标应用程序实时运行时所调用的特定 Android API，并对日志内容进行详细说明，便于日志匹配；然后将日志发送到匹配模块进行分析。2）匹配模块：该模块离线运行，通过从日志模块接收的日志显示应用程序行为的上下文信息。根据日志信息，从应用市场或互联网获取 APK 文件，以实现日志匹配。具体匹配过程如下：首先对应用程序代码和日志进行预处理，分别输出超图和日志段；然后，超图将控制流图（CFGs）和应用程序的调用流程图结合在一起；接下来，它将每个与日志记录匹配的日志点单独定位在相应的超图上，并探索这些连接日志点的路径；根据所连接的日志路径，最后判断当前的应用程序运行是否为合法功能的启动。

然而，与隐藏功能不同，窃听行为很可能被正常行为掩盖，导致这些工具的有效性降低。此外，麦克风的未授权访问行为可能是由开发人员的错误逻辑引起的，在此情况下通过后门分析难以发现。

3.4 基于麦克风状态显示的方法

Android 系统的开发者提出显示麦克风的状态，以便用户判断麦克风访问行为是否属于窃听。具体而言，Android 9.0，Android 10.0 和 Android 11.0 分别在通知栏[55-56]、状态栏[57-60]、日志文件[59]添加了通知，当麦克风被占用时，麦克风图标分别显示在状态栏和通知栏中。Android 12.0 则会点亮麦克风图标[34]，并在使用麦克风时显示使用该麦克风的应用程序的名称。然而，这些通知不仅很容易被忽略和混淆，而且只能显示麦克风的状态，不能识别窃听攻击。

为解决无法识别窃听攻击以及麦克风状态的显示易被混淆和遮挡的问题，Huang 等[58]提出了窃听检测方案 MicID。该方案通过分析安卓系统中移动应用程序访问麦克风的方式和调用流程，明确了用户触碰屏幕是授权麦克风访问的重要行为。因此提出，在麦克风被调用时，判断是否存在用户触碰屏幕的行为，从而实现有效地窃听攻击检测。此外，该方案还设计了新颖的悬浮窗，当识别到窃听行为时，悬浮窗以不可点击的方式出现在屏幕中间；当无窃听行为发生时，悬浮窗透明，不影响用户对屏幕的正常感知。MicID 窃听有效性虽然能达到 91%，但是其仅适用于通过触屏方式授权访问麦克风的应用程序的窃听判断，对通过语音指令唤醒的语音助手则无效。

3.5 存在的不足及挑战

已有研究虽然从多角度抵御语音助手的窃听行为，以保护用户隐私，但这些方法依然存在使用场景单一和无法自动检测窃听行为等主要局限。

1）通用性不足：基于流量分析的方法和基于侧信道的方法仅适用于使用语音唤醒且网络流量单一的智能家居设备。然而，移动应用程序的语音助手并非持续在线，并且移动设备因搭载诸多移动应用程序使得网络流量复杂，此时音频流量难以被捕获和分析。

2）有效性不足：基于源码审查的方法虽然可以识别出未向用户披露的隐藏行为，但是当麦克风的未授权访问行为属于逻辑上的设计缺陷或恶意修改时，这类方法的有效性将会大大降低。基于麦克风状态显示的方法虽然能够显示麦克风正在被占用，但无法自动判断当前的占用行为是否合法。

通过对上述防御方案的分析可知，如何根据麦克风的调用模式，有效区分当前麦克风的访问是否由用户的正常授权而产生，是实现通用且有效的窃听攻击检测需要解决的重大挑战。

4 未来方向展望与挑战分析

综上所述，语音助手的窃听攻防研究已成为当前信息安全领域的研究重点。国内外的研究学者虽然从多个角度实施语音窃听攻击来探索语音助手的安全漏洞，并提出了一些类防御方案来保护语音交互中的用户隐私，但是这些研究忽略了语音助手的唤醒需要用户授权的特点，导致窃听行为不隐蔽和防御方案通用性不足。因此，针对语音助手的窃听攻击与防御问题，未来可从以下两方面进一步展开深入探索。

1）隐蔽的语音窃听攻击。依据语音助手的唤醒方式来研究隐蔽的窃听攻击，并揭露语音助手的安全与隐私漏洞，仍是值得研究者进行深入探索的方法。

针对 2.4 节所总结的现有窃听攻击研究存在的攻击隐蔽性不足、通用性不足、攻击实施难度高的问题，未来研究的问题、挑战及研究思路如表 3 所列。

2）通用且有效的窃听攻击检测。根据语音助手的唤醒模式，实现有效且通用的窃听防御方案，对推进语音助手产业的可持续性发展、保护用户的语音安全与隐私具有重要研究意义和实际应用价值，且该领域仍具有十分广阔的研究空间。

针对 3.5 节所总结的现有窃听防御研究存在的窃听识别通用性不足、有效性不足的问题，未来研究的问题、面临的挑战及研究思路如表 4 所列。

表 3 语音窃听攻击的未来研究问题、挑战与思路

Table 3 Future research problems, challenges and ideas of voice eavesdropping attack

研究问题	研究挑战	研究思路
如何揭示不同设备间语音助手之间的关联，实现通用窃听攻击？	设备多样性：不同设备的语音助手实现方式各异，缺乏统一标准 跨平台兼容性：攻击方法难以同时适用于多种语音助手和设备	跨平台攻击框架：研究不同语音助手的共性，开发适用于多种设备和语音助手的通用攻击框架 标准化漏洞利用：探索语音助手 API 的标准化漏洞，设计能够绕过设备差异的攻击方法 多语言支持：研究支持多语言的攻击方法，确保攻击在不同语言环境下均能实施
如何遵循语音助手固有的唤醒模式隐藏窃听行为？	用户感知：传统语音命令容易被用户察觉 隐蔽性不足：现有攻击方法容易被安全系统检测到	无声攻击：利用超声波或其他不可听频率的信号进行攻击，避免用户感知 环境噪声伪装：将攻击信号伪装成环境噪声，降低被检测的可能性 多模态攻击：结合视觉、触觉等其他感官输入，设计多模态攻击方式，增强隐蔽性
如何降低攻击实施难度？	技术门槛高：现有攻击方法需要精准的信号设计和复杂的设备配置 环境依赖性：攻击效果易受环境干扰	自动化攻击工具：开发自动化工具，简化攻击信号的生成和发射过程 自适应攻击策略：研究自适应攻击策略，使攻击能够根据环境变化自动调整信号参数 低成本攻击设备：设计低成本、易获取的攻击设备，降低攻击实施的技术门槛

表 4 语音窃听防御的未来研究问题、挑战与思路

Table 4 Future research problems, challenges and ideas of voice eavesdropping defense

研究问题	研究挑战	研究思路
如何挖掘不同授权语音助手唤醒行为的统一模式？	授权方式多样：不同设备的语音助手唤醒方式各异（如语音指令、触屏操作等） 行为模式复杂：难以提取统一的唤醒行为特征	多维度行为分析：结合用户语音指令、触屏操作等多种授权行为，挖掘统一的唤醒模式 机器学习模型：利用机器学习技术，训练模型识别不同设备的授权行为共性 跨设备行为关联：研究不同设备间用户授权行为的关联性，设计通用的检测机制
如何提高防御方法的通用性？	场景多样性：不同设备和网络环境的复杂性导致防御方法难以通用 跨平台兼容性：现有防御方法难以同时适用于多种语音助手和设备	跨平台防御框架：开发适用于多种语音助手和设备的通用防御框架 多场景适应性：研究能够适应不同网络环境和设备类型的防御方法 多语言支持：设计支持多语言的防御机制，确保在不同语言环境下仍能有效识别窃听行为
如何提高防御方法的有效性？	检测精度不足：现有防御方法在识别窃听行为时存在漏报和误报 实时性不足：难以在窃听攻击发生时迅速检测并响应	多维度检测：结合流量分析、侧信道分析和行为分析，设计多维度的检测机制 实时监控与响应：开发实时监控系统，能够在窃听攻击发生时迅速检测并响应 隐私保护技术：研究如何在防御过程中保护用户隐私，避免泄露敏感信息
如何改进麦克风状态显示与用户交互？	用户感知不足：现有麦克风状态显示方式容易被忽略或混淆 交互体验不佳：用户难以快速识别麦克风的异常使用	增强显示效果：设计更加醒目和直观的麦克风状态显示方式 智能提示与反馈：开发智能提示系统，根据用户的使用习惯和环境变化提供个性化提示 用户教育与意识提升：通过教育和宣传，提高用户对麦克风使用状态的认识
如何应对新型攻击方式？	新型攻击威胁：未来可能出现利用零日漏洞或物理层信号的新型攻击 防御滞后性：现有防御方法难以应对未知攻击方式	零日漏洞防御：研究如何防御利用语音助手零日漏洞的新型攻击 物理层防御：探索利用物理层信号（如电磁波、光信号）进行防御的可能性 社交工程防御：结合社交工程手段，设计更加隐蔽和高效的防御方式

结束语 最近研究表明，语音助手在提供便捷语音交互的同时，也存在窃听用户对话、泄露用户隐私的风险。本文首先根据窃听攻击的实施方式，较为全面地对近十年来有关语音窃听攻击的方法进行总结并分为 3 类，并对每个类别的攻击方法进行详细分析与讨论。然后，本文系统地回顾了近年来有关窃听防御的研究对策，并将其根据实现原理分类为 4 个主要类别，通过对每个类别的防御对策进行详细分析，归纳出其存在的不足之处及挑战。最后，本文分别讨论了语音窃听攻击和防御两个方面的未来研究方向以及面临的挑战。

综上所述，研究面向语音助手的窃听攻击与防御，对于揭露语音交互过程中的安全与隐私风险、保护用户安全与隐私、构建更加安全可靠的语音助手系统，以及促进语音交互应用的可持续发展具有重要的意义。

参 考 文 献

[1] ZHANG J, LI H, ZHANG S M, et al. Review of Pre-training Methods for Visually-rich Document Understanding[J]. Computer Science, 2025, 52(1): 259-276.

[2] QIU J，HAN R，WEI Z F，et al. Research of public infrastructure system and security policy in cyberspace[J]. Chinese Journal of Network and Information Security，2021，7(6)：56-67.

[3] ZHANG R，JIANG C，WU S，et al. Wi-Fi sensing for joint gesture recognition and human identification from few samples in human-computer interaction[J]. IEEE Journal on Selected Areas in Communications，2022，40(7)：2193-2205.

[4] WANG L，CHEN M，LU L，et al. VoiceListener：A Training-free and Universal Eavesdropping Attack on Built-in Speakers of Mobile Devices[C]// Proceedings of the ACM on Interactive，Mobile，Wearable and Ubiquitous Technologies. 2023：1-22.

[5] REN K，MENG Q R，YAN S K，et al. Survey of artificial intelligence data security and privacy protection[J]. Chinese Journal of Network and Information Security，2021，7(1)：1-10.

[6] SHEN X C，GE Y H，CHEN B，et al. Research on construction technology of artificial intelligence security knowledge graph [J]. Chinese Journal of Network and Information Security，2023，9(2)：164-174.

[7] ZHANG R，ZHANG P Y，SUN C L. Speech enhancement method based on multi-domain fusion and neural architecture search[J]. Journal on Communications，2024，45(2)：225-239.

[8] CHIN J，DESAI S，LIN S，et al. Like my aunt dorothy：effects of conversational styles on perceptions，acceptance and metaphorical descriptions of voice assistants during later adulthood[C]// Proceedings of the ACM on Human-Computer Interaction. 2024：1-21.

[9] WANG A H，ZHANG L，SONG W，et al. Review of End-to-End Streaming Speech Recognition[J]. Computer Engineering and Applications，2023，59(2)：22-33.

[10] JIANG Y，LI W，HOSSAIN M S，et al. A snapshot research and implementation of multimodal information fusion for data-driven emotion recognition[J]. Information Fusion，2020，53：209-221.

[11] MENG Y，LI S F，ZHANG Y C，et al. Information Physical Integration System Security for Smart Home Platform[J]. Computer Research and Development，2019，56(11)：2349-2364.

[12] WALKER P，SAXENA N. Evaluating the effectiveness of protection jamming devices in mitigating smart speaker eavesdropping attacks using gaussian white noise[C]// Proceedings of the 37th Annual Computer Security Applications Conference. 2021：414-424.

[13] ZHU H，WANG X，JIANG Y，et al. Secure Voice Interactions With Smart Devices[J]. IEEE Transactions on Mobile Computing，2021，22(1)：515-526.

[14] WANG C，XIE L，LIN Y，et al. Thru-the-wall eavesdropping on loudspeakers via RFID by capturing sub-mm level vibration [C]// Proceedings of the ACM on Interactive，Mobile，Wearable and Ubiquitous Technologies. 2021：1-25.

[15] CHENG L，WILSON C，LIAO S，et al. Dangerous skills got certified：Measuring the trustworthiness of skill certification in voice personal assistant platforms[C]// Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. 2020：1699-1716.

[16] EDU J S，SUCH J M，SUAREZ-TANGIL G. Smart home personal assistants：a security and privacy review[J]. ACM Computing Surveys(CSUR)，2020，53(6)：1-36.

[17] QIN Y，YU C，LI Z，et al. Proximic：Convenient voice activation via close-to-mic speech detected by a single microphone[C]// Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. 2021：1-12.

[18] YAN C，JI X，WANG K，et al. A survey on voice assistant security：Attacks and countermeasures[J]. ACM Computing Surveys，2022，55(4)：1-36.

[19] WANG Z，LIU D，SUN Y，et al. A survey on IoT-enabled home automation systems：Attacks and defenses[J]. IEEE Communications Surveys & Tutorials，2022，24(4)：2292-2328.

[20] LI J，CHEN C，AZGHADI M R，et al. Security and privacy problems in voice assistant applications：A survey[J]. Computers & Security，2023，134：103448.

[21] HUANG W，TANG W，JIANG H，et al. Stop deceiving! an effective defense scheme against voice impersonation attacks on smart devices[J]. IEEE Internet of Things Journal，2021，9(7)：5304-5314.

[22] REN Y，PENG H，LI L，et al. Generalized voice spoofing detection via integral knowledge amalgamation[C]// IEEE/ACM Transactions on Audio，Speech，and Language Processing. 2023：2461-2475.

[23] CHEN M，LU L，WANG J，et al. VoiceCloak：Adversarial Example Enabled Voice De-Identification with Balanced Privacy and Utility[C]// Proceedings of the ACM on Interactive，Mobile，Wearable and Ubiquitous Technologies. 2023：1-21.

[24] WANG P，GAO H C，GUO X Y，et al. Improving the security of audio captchas with adversarial examples[J]. IEEE Transactions on Dependable and Secure Computing，2023，21(2)：650-667.

[25] JANG Y，SONG C，CHUNG S P，et al. A11y attacks：Exploiting accessibility in operating systems[C]// Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. 2014：103-115.

[26] ZHANG R，CHEN X，WEN S，et al. Who activated my voice assistant? A stealthy attack on android phones without users' awareness[C]// Machine Learning for Cyber Security. Cham：Springer，2019：378-396.

[27] ESPOSITO S，SGANDURRA D，BELLA G. Alexa versus alexa：Controlling smart speakers by self-issuing voice commands [C]// Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security. 2022：1064-1078.

[28] HUANG W，CHEN H，CAO H，et al. Manipulating Voice Assistants Eavesdropping via Inherent Vulnerability Unveiling in Mobile Systems[J]. IEEE Transactions on Mobile Computing，2024，23(12)，11549-11536.

[29] ZHANG G，YAN C，JI X，et al. Dolphinattack：Inaudible voice commands[C]// Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017：103-117.

[30] ROY N，SHEN S，HASSANIEH H，et al. Inaudible voice commands：The {Long-Range} attack and defense[C]// 15th USENIX Symposium on Networked Systems Design and Implementation(NSDI 18). 2018：547-560.

[31] MICHALEVSKY Y，BONEH D，NAKIBLY G. Gyrophone：Recognizing speech from gyroscope signals[C]// 23rd USENIX Security Symposium(USENIX Security 14). 2014：1053-1067.

[32] BA Z，ZHENG T，ZHANG X，et al. Learning-based Practical Smartphone Eavesdropping with Built-in Accelerometer[C]// NDSS. 2020：1-18.

[33] GAO M，LIU Y，CHEN Y，et al. Device-independent Smartphone Eavesdropping Jointly using Accelerometer and Gyroscope[J]. IEEE Transactions on Dependable and Secure Compu-

ting, 2022, 20(4): 3144-3157.
[34] WANG L, CHEN M, LU L, et al. VoiceListener: A Training-free and Universal Eavesdropping Attack on Built-in Speakers of Mobile Devices[C]// Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies. 2023: 1-22.
[35] ZHANG S, LIU Y, GOWDA M. I spy you: Eavesdropping continuous speech on smartphones via motion sensors[C]// Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies. 2023: 1-31.
[36] CHEN H, JIN W, HU Y, et al. Eavesdropping on Black-box Mobile Devices via Audio Amplifier's EMR[C]// Proceedings of the 2018 Annual International Conference on Network and Distributed System Security(NDSS). 2024.
[37] LIAO Q, HUANG Y, HUANG Y, et al. An eavesdropping system based on magnetic side-channel signals leaked by speakers [J]. ACM Transactions on Sensor Networks, 2024, 20(2): 1-30.
[38] ZHU X, WANG W G, WANG J Y, et al. Just-In-Time Software Defect Prediction Approach Based on Fine-grained Code Representationand Feature Fusion [J]. Computer Science, 2025, 52(1): 242-249.
[39] LI J Q, LIU W P, HUANG D, et al. Multimodal Fusion Based Dynamic Malware Detection [J]. Computer Science, 2024, 51(S2): 946-952.
[40] DIAO W, LIU X, ZHOU Z, et al. Your voice assistant is mine: How to abuse speakers to steal information and control your phone[C]// Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices. 2014: 63-74.
[41] ZHANG R, CHEN X, LU J, et al. Using AI to hack IA: A new stealthy spyware against voice assistance functions in smart phones[J]. arXiv: 1805.06187, 2018.
[42] HUANG W, TANG W, ZHANG K, et al. Thwarting unauthorized voice eavesdropping via touch sensing in mobile systems [C]// IEEE INFOCOM 2022-IEEE Conference on Computer Communications. 2022: 31-40.
[43] WANG X, CONTINELLA A, YANG Y, et al. Leakdoctor: Toward automatically diagnosing privacy leaks in mobile applications[C]// Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies. 2019: 1-25.
[44] ZHOU R, JI X, YAN C, et al. DeHiREC: Detecting Hidden Voice Recorders via ADC Electromagnetic Radiation[C]// 2023 IEEE Symposium on Security and Privacy (SP). IEEE, 2023: 3113-3128.
[45] AHMED D, SABIR A, DAS A. Spying through your voice assistants: realistic voice command fingerprinting[C]// 32nd USENIX Security Symposium (USENIX Security 23). 2023: 2419-2436.
[46] MITEV R, PAZII A, MIETTINEN M, et al. Leakypick: Iot audio spy detector[C]// Annual Computer Security Applications Conference. 2020: 694-705.
[47] ZHU D, JIN H, LIU Y, et al. PhoneCheck: App-level protection against eavesdropping on Android[C]// 2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN). IEEE, 2017: 686-693.
[48] SUN K, CHEN C, ZHANG X. " Alexa, stop spying on me!" speech privacy protection against voice assistants[C]// Proceedings of the 18th Conference on Embedded Networked Sensor Systems. 2020: 298-311.
[49] ZHAO Q, ZUO C, DOLAN-GAVITT B, et al. Automatic uncovering of hidden behaviors from input validation in mobile apps[C]// IEEE Symposium on Security and Privacy (SP). IEEE, 2020: 1106-1120.
[50] MENG Z, XIONG Y, HUANG W, et al. AppAngio: Revealing Contextual Information of Android App Behaviors by API-Level Audit Logs [J]. IEEE Transactions on Information Forensics and Security, 2020, 16: 1912-1927.
[51] FRATANTONIO Y, BIANCHI A, ROBERTSON W, et al. Triggerscope: Towards detecting logic bombs in android applications[C]// IEEE Symposium on Security and Privacy (SP). IEEE, 2016: 377-396.
[52] SENANAYAKE J, KALUTARAGE H, AL-KADRI M O, et al. Android source code vulnerability detection: a systematic literature review[J]. ACM Computing Surveys, 2023, 55(9): 1-37.
[53] XU K, LI Y, DENG R H. Iccdetector: Icc-based malware detection on android[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(6): 1252-1264.
[54] WONG M Y, LIE D. Intellidroid: a targeted input generator for the dynamic analysis of android malware[C]// NDSS. 2016: 21-24.
[55] LEE Y T, ENCK W, CHEN H, et al. PolyScope: Multi-Policy Access Control Analysis to Compute Authorized Attack Operations in Android Systems[C]// USENIX Security Symposium. 2021: 2579-2596.
[56] WANG S, LING Z, ZHANG Y, et al. Implication of animation on Android security[C]// 2022 IEEE 42nd International Conference on Distributed Computing Systems(ICDCS). IEEE, 2022: 1122-1132.
[57] ZOUHAIER L, BENDALYHLAOUI Y, AYED L B. Adaptive user interface based on accessibility context [J]. Multimedia Tools and Applications, 2023, 82: 35621-35650.
[58] HUANG W, TANG W, CHEN H, et al. Unauthorized Microphone Access Restraint Based on User Behavior Perception in Mobile Devices[J]. IEEE Transactions on Mobile Computing, 2024, 23(1): 955-970.
[59] HUANG W, TANG W, JIANG H, et al. Recognizing Voice Spoofing Attacks Via Acoustic Nonlinearity Dissection for Mobile Devices [J]. IEEE Transactions on Mobile Computing, 2024, 23(12), 12080-12096.
[60] CAO H, HUANG W, XU G, et al. Security analysis of wifi-based sensing systems: Threats from perturbation attacks[J]. arXiv: 2404.15587, 2024.

HUANG Wenbin, born in 1995, associate professor. His main research interests include smart sensing security, mobile system security, artificial intelligence and its application security.

XIONG Lizhi, born in 1988, professor. His main research interests include artificial intelligence and security, multimedia information security, adversarial attack and defense.

(责任编辑:喻藜)